

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)
(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No. COS99070

Total Pages in this Submission

52

1589 U.S. PTO
09/627558
07/28/00

TO THE ASSISTANT COMMISSIONER FOR PATENTS
Box Patent Application
Washington, D.C. 20231

Transmitted herewith for filing under 35 U.S.C. 111(a) and 37 C.F.R. 1.53(b) is a new utility patent application for an invention entitled:

SECURE TRANSACTION CARD USING BIOMETRICAL VALIDATION

and invented by: Thomas J. Herder

If a CONTINUATION APPLICATION, check appropriate box and supply the requisite information:

Continuation Divisional Continuation-In-Part of prior application No.: _____

Which is a:

Continuation Divisional Continuation-In-Part of prior application No.: _____

Which is a:

Continuation Divisional Continuation-In-Part of prior application No.: _____

Enclosed are:

Application Elements

1. Filing fee as calculated and transmitted as described below

2. Specification having 38 pages and including the following:
 - a. Descriptive Title of the Invention
 - b. Cross Reference to Related Applications (*if applicable*)
 - c. Statement Regarding Federally sponsored Research/Development (*if applicable*)
 - d. Reference to Microfiche Appendix (*if applicable*)
 - e. Background of the Invention
 - f. Brief Summary of the Invention
 - g. Brief Description of the Drawings (*if drawings filed*)
 - h. Detailed Description
 - i. Claim(s) as Classified Below
 - j. Abstract of the Disclosure

07/28/00
JC892 U.S. PTO

07-31-00

Docket No. COS99070

Total Pages in this Submission 52

07/28/00
JC892 U.S. PTO

NEW UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)
(Only for new nonprovisional applications under 37 CFR 1.53(b))

Application Elements (continued)

3. **■ Drawing(s) (when necessary as prescribed by 35 USC 113)**

Formal Informal Number of Sheets 7

4. **■ Oath or Declaration**

a. Newly Executed b. Unexecuted c. With Power of Attorney d. Without Power of Attorney
e. Copy from a prior application (37 CFR 1.63(d)) (for continuation/divisional application only)

DELETION OF INVENTORS(S)

Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. 1.63 (d)(2) and 1.33 (b).

5. **Incorporation By Reference (usable if Box 4e is checked)**

The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4e, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. Computer Program in Microfiche (Appendix)

7. Nucleotide and/or Amino Acid Sequence Submission (if applicable, all must be included)

a. Paper Copy

b. Computer Readable Copy (identical to computer copy)

c. Statement Verifying Identical Paper and Computer Readable Copy

Accompanying Application Parts

8. Assignment Papers (cover sheet and document(s))

9. 37 CFR 3.73(b) Statement (where there is an assignee)

10. English translation Document (if applicable)

11. Information Disclosure Statement/PTO 1449 Copies of IDS Citations

12. Preliminary Amendment

13. Acknowledgment postcard

14. Certificate of Mailing

First Class

Express Mail

EL 479596659US

NEW UTILITY PATENT APPLICATION TRANSMITTAL
 (Large Entity)
(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No. COS99070

Total Pages in this Submission 52

15. Certified Copy of Priority Document(s) (if foreign priority is claimed)

16. Additional Enclosures (please identify):

Fee Calculation and Transmittal

CLAIMS AS FILED

For	# Filed	# Allowed	# Extra	Rate	Fee
Total Claims	22	-20 =	2	x \$18.00	\$ 36.00
Indep. Claims	4	- 3 =	1	x \$78.00	\$ 78.00
Multiple Dependent Claims (check if applicable)					\$ 0.00
				BASIC FEE	\$ 690.00
OTHER FEE (specify purpose)					
				TOTAL FILING FEE	\$ 804.00

A check in the amount of _____ to cover the filing fee is enclosed.

The Commissioner is hereby authorized to charge and credit Deposit Account No. 13-2491 as described below. A duplicate copy of this sheet is enclosed.

- Charge the amount of \$804.00 as filing fee.
- Charge the amount of \$40.00 as the Assignment Recordation Fee.
- Credit any overpayment.
- Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
- Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).

Dated:

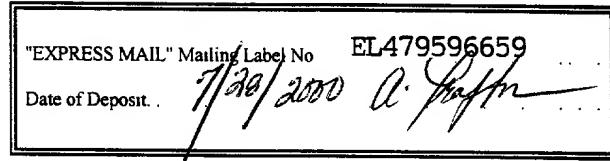


Carl J. Evans
 Attorney for applicant(s)
 Registration No.: 33,874

cc:

Send all correspondence to:
 Technology Department
 MCI WORLDCOM, Inc.
 1133 19th STREET, NW
 WASHINGTON, DC 20036

PATENT APPLICATION
DOCKET NO.: 1275-0006
COS-99-070



SECURE TRANSACTION CARD USING BIOMETRICAL VALIDATION

5 BACKGROUND OF THE INVENTION

Technical Field of the Invention

10 The present invention relates generally to access control systems and methods, and more particularly, to a secure transaction card, e.g., a calling card, that uses biometric profiling for validation and access control.

Description of Related Art

Access control schemes are a key component in today's fraud detection systems used with respect to transactions that involve a

transaction card and the like. For example, as is well known, calling or phone cards, credit cards, Automated Teller Machine (ATM) cards or debit cards, et cetera, typically require entering a correct Personal Identification Number (PIN) as an access control mechanism. To further increase security, some transaction cards have an integrated circuit (e.g., 5 Smart Cards) which facilitates encryption of a legitimate cardholder's personal identity information and other data.

Although there have been impressive advances in the existing access control schemes designed to reduce costs to a card-issuing entity 10 and its customers, current solutions are not entirely satisfactory. First, there is no sure way that any current system can guard against all forms of fraud, and there is no tangible means of determining what the actual fraud costs are. Moreover, the same technological advances that have increased security by means of encryption are also making it possible for 15 illegitimately deciphering access codes etc.

In addition, current access control schemes are typically static, i.e., the same access code is used for each and every transaction by a user and, accordingly, the same verification scheme is also employed by the fraud detection system associated therewith. Thus, the probability of a 20 successful attack by an unauthorized party to decipher an access code or password increases, thereby rendering the system vulnerable.

Those skilled in the art should appreciate that despite various improvements, transaction card-related fraud is still possible primarily because of two factors. First, cards and their PINs can still be easily stolen or misplaced. And, second, any access control scheme used in connection with a card can be reverse-engineered with luck and perseverance because the devices used as access control “gatekeepers” are typically alphanumeric codes, passwords, and the like which lend themselves to reproduction by somebody who does not own them.

10 **SUMMARY OF THE INVENTION**

Accordingly, the present invention is directed to a method of validating a user for a transaction based on biometric profiling that is inherently and uniquely coupled to the user such that reproducing a correct response required for access control by an unauthorized party is virtually impossible. Initially, a biometric profile is configured for the user, which includes a plurality of biometric samples relating to the user such as, e.g., voice responses to personalized questions, et cetera. The biometric profile is associated with an indicium (e.g., Personal Identification Number, card number, user name, etc.) assigned to the transaction card. When a transaction is attempted by the user at a terminal, the user is biometrically interrogated by the system which directs a question that is randomly selected from the plurality of

questions used in the configuration process. Thereafter, the biometric response (e.g., voiceprint) generated with respect to the user in response to the step of biometrical interrogation is monitored in order to determine if the biometric response matches a biometric sample in the biometric profile of the user. If so, the user is approved for the transaction and access is accordingly provided.

In another aspect, the present invention is directed to a method of validating a user for a call to be effectuated over a Public Switched Telephone Network (PSTN) using a calling card. The validation method commences by configuring a personalized profile for the user, wherein the personalized profile includes a plurality of voice samples elicited from the user in response to a plurality of personalized questions directed to the user. Thereafter, the personalized profile is associated with an indicium assigned to the calling card. When a calling card transaction is attempted by the user, a determination is made if a voice verification is needed with respect to the user. If so, the user is queried by an Automated/Audio Response Unit (ARU) for a voice response to a question that is randomly selected from the plurality of personalized questions used in the configuration process. Thereafter, the voice response is verified to determine if it matches a corresponding voice sample in the voice profile of the user. If so, the user is approved for the calling card transaction.

In yet another aspect, the present invention is directed to a fraud prevention method for use in a transaction-card-based system having a conventional authentication process. The method involves first determining, by utilizing the conventional authentication process, if a 5 fraudulent transaction is being attempted in the transaction-card-based system by a user using a transaction card. If so, the user is then biometrically interrogated in order to obtain a biometric sample from the user. The biometric sample is monitored whereby the user is denied access for the transaction in the transaction-card-based system if the 10 biometric sample does not match an entry stored in a biometric profile database having information that is inherently associated with the transaction card's owner.

In yet further aspect, the present invention is directed to an access control system for use with a transaction-card-based scheme. The access 15 control system comprises a network operable with a terminal used for interacting with a user in association with a transaction card. A controller is disposed in the network to query the user when the user attempts a transaction using the transaction card. A secure access server is disposed in the network, which responds to messages from the 20 controller with respect to querying the user. A profile database is coupled to the server, which includes a plurality of biometric samples inherently coupled to the user. The biometric samples are associated with an

indicium assigned to the transaction card such that when the user attempts the transaction, the controller queries the user for a response thereto. If the response does not match a corresponding entry in the profile database, the user is denied access for the transaction.

5

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of the present invention may be had by reference to the following Detailed Description when taken in conjunction with the accompanying drawings wherein:

10 FIG. 1 depicts a functional block diagram of a network system provided in accordance with the teachings of the present invention for biometrically validating a user for a transaction;

15 FIG. 2 depicts a flow chart of the steps of an exemplary embodiment of the biometrical validation scheme of the present invention;

FIG. 3 is a functional block diagram of a presently preferred exemplary embodiment of the present invention which utilizes a voice-based validation method;

20 FIGS. 4A - 4C depict a flow chart of a presently preferred exemplary embodiment of the voice-based validation method provided in accordance with the teachings of the present invention; and

FIG. 5 depicts a flow chart of a voice profile configuration process for use in the voice-based validation method of the present invention.

DETAILED DESCRIPTION OF THE DRAWINGS

5 In the drawings, like or similar elements are designated with identical reference numerals throughout the several views, and the various elements depicted are not necessarily drawn to scale. Referring now to FIG. 1, depicted therein is a functional block diagram of an exemplary communications system 100 provided in accordance with the teachings of the present invention for biometrically validating a user with respect to an on-line transaction to be effectuated using a transaction card such as, for example, a calling card or phone card, etc. A network 102 is included in the system 100 to exemplify a heterogeneous inter-networking environment which may include any combination of the following network portions: a wireline telecommunications network (i.e., the Public Switched Telephone Network or PSTN), one or several wireless telecommunications networks operating with known protocols, e.g., Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA), Global System for Mobile Communications (GSM), Multi-point Microwave Distribution System (MMDS), etc., and may also comprise an Internet Protocol (IP)-based packet-switched network (PSN) portion for providing Voice-over-IP (VoIP) telephony, e.g., an H.323

10

15

20

network or a Session Initiation Protocol (SIP) network, or the Internet. Those skilled in the art should further appreciate that the network 102 is also illustrative and inclusive of any proprietary or customized operator networks used for data transport, e.g., Local Area Networks (LANs),
5 Wide Area Networks (WANs), Metropolitan Area Networks (MANs), Ethernet portions, Token Ring portions, etc., which interconnect the various nodes and equipment used for effectuating the biometrical validation scheme of the present invention, as will be described in greater detail hereinbelow.

10 A plurality of telecommunications devices, e.g., Internet phones, SIP phones, H.323 terminals, Information Appliances, POTS wireline phones, mobile stations, computers having suitable Telephony Application Programming Interfaces (TAPIs), etc., collectively referred to as "terminals" hereinafter, are provided in the network system 100 such that a user/subscriber may place a call, engage in a transaction, or otherwise interact with the network system, using an appropriate terminal and the transaction card issued to the user. Furthermore, in accordance with the teachings of the present invention, the terminals are provided with the capability to capture the user's biometric responses, e.g., voice,
15 ocular, or other biometric patterns, etc., in addition to keypad inputs such as Dual Tone Multi-Frequency (DTMF) codes. Four terminals, T 104A - T 104D, are exemplified in FIG. 1, wherein the user 106 interacts with
20

T 104B with respect to an on-line transaction. A controller 120 interacts with a secure card server 108 provided in the network system 100, which is coupled to a biometric profile database 110, for the purpose of validating the user 106 when the user attempts to engage in the on-line 5 transaction using the transaction card.

FIG. 2 depicts a flow chart of the steps of an exemplary embodiment of the biometrical validation scheme in general operation. During initialization, a biometric profile is created or configured for the user, either on-line or off-line, by obtaining a plurality of biometric samples relating to the user (step 202). For example, such samples may comprise voice responses provided by the user in response to personalized questions that the user is required to answer during the configuration process. Preferably, the profile may be defined via a menu of selectable and/or prompted options that require personalized input such as: user name, indicia, e.g., Personal Identification Number (PIN) or card number and the like, and personal data such as age, weight, Social Security Number, maiden name, nick name(s), hobby(ies), favorite movie/star/celebrity, favorite book/music/band, most favorite scientist/politician, blood type, etc. For the purposes of biometric profiling, user responses are preferably provided as voice inputs, although it should be apparent that DTMF key codes may also be provided as a further embodiment. Accordingly, the profile database 110 10 15 20

(shown in FIG. 1) may comprise both non-DTMF responses and DTMF responses in certain implementations.

Similarly, other biometric parameters or patterns may be profiled for the user in the configuration process (step 202). Fingerprinting, 5 facial pattern recognition, retinal signatures, etc. may be used for populating the biometric profile database in conjunction with voice and DTMF key inputs.

Thereafter, as indicated in step 204, an association is made in the network system 100 (shown in FIG. 1) between the user profile data 10 (DTMF and non-DTMF) and the transaction card issued to the user by an authorized entity, e.g., Government agencies (access cards), telephone companies (Telcos) (calling cards), credit card companies, credit bureaus (access to credit reports), financial institutions such as banks, credit unions (account access cards), Internet businesses or e-commerce entities 15 (secure access), companies providing employee access to corporate or personal information or services, and the like. It should be realized by those skilled in the art that by making the association between the personalized responses (i.e., profiles and samples therein) and the transaction card in accordance with the teachings of the present 20 invention, an inherent and intimate bonding is achieved between the card and the user such that it thwarts fraudulent/unauthorized use of the transaction card. Accordingly, the user does not have to worry about

losing a card, remembering a PIN, or having to conceal a card number and the PIN associated therewith.

When a card-related transaction is attempted by the user using a suitable terminal (such as T 104B illustrated in FIG. 1) (decision block 206), a determination is made in the network system 100 (e.g., controller 120) whether a profile-based validation is required for the transaction card (decision block 208). If the profile-based validation is not required, the biometrical validation scheme of the present scheme may terminate (step 218) or, in some exemplary embodiments, may continue with other authentication schemes using PINs, DTMF inputs, etc. Also, it should be apparent that such non-biometric authentication procedures may be used in conjunction with the biometrical validation process provided in accordance herewith.

Continuing to refer to FIG. 2, after determining that a profile-based validation is required for the transaction card, an appropriate network entity queries the user for a biometric printing (step 210). For example, for a voice-based profile validation, a question may be randomly selected from the questions that were used in the profile configuration process and be directed to the user for a response. By speaking the answer into the terminal, a unique voiceprint response is obtained, which is subsequently matched with the corresponding sample in the profile database (decision block 212). Those skilled in the art

should realize that more than one sample may be provided in the profile database for a particular question such that a range may be provided therewith, and any normal variations in the response may be accounted for accordingly.

5 If there is no match found between the response and the sample, access may be denied to the user for that transaction (step 216). On the other, access is provided where there is a match (step 214) so that the user may proceed with the transaction. Thereafter, the biometrical validation scheme may cease (step 218), unless further transaction 10 sessions are engaged. That is, once authorized for a session, re-validation is not required. Once again, a non-biometric authentication procedure may be employed in conjunction with the present scheme whether or not access is provided based on the profile validation process.

15 Referring now to FIG. 3, depicted therein is a functional block diagram of a presently preferred exemplary embodiment of a voice-based validation scheme for use in a hybrid telecommunications network 300 having a PSTN portion 302 and a PSN portion 338. A plurality of wireline phones, e.g., PH 304A - PH 304C, are conventionally provided with respect to the PSTN portion 302. A bridging switch 306 is connected to the PSTN 302, which sends calls to an Automated Call 20 Distributor (ACD) 308 based upon call association. The ACD 308 routes the calls based upon its configuration information, and in conjunction

with an Intelligent Services Network Adjunct Processor (ISNAP) acting as a signaling gateway (e.g., ISNAP 310A and ISNAP 310B), to a suitable application platform, which comprises an Automated/Audio Response Unit (ARU) 322 or a Manual Telecom Operator Console (MTOC) 328. It should be readily apparent to those skilled in the art that ARU and MTOC, which may be co-located or placed separately, form a Call Center of a service provider. One or more corporate/private Ethernet portions, e.g., Ethernet 314A and Ethernet 314B, may typically be provided at the Call Center (also referred to as the Operator Center sometimes) for furnishing connectivity between the ISNAP elements and the application platforms (i.e., ARU 322 and MTOC 328). It is also possible that these application platforms may be located on different LAN segments at the same site, or may be located at different sites and a WAN 316 may be suitably provided therebetween for data link connectivity.

Continuing to refer to FIG. 3, the ACD operates as a switching system designed to queue and/or distribute a large volume of incoming calls to the next available “answering position,” whereby calls are categorized by the calling number and are directed to the appropriate processing entity. The ARU functions as a type of automated operator console, comprising an Automated Call Processor (ACP) 326 and a Network Information Distributed Services (NIDS) Audio Server (NAS)

324. ACP 326 processes the calls and works in cooperation with NAS
324 which provides voice scripting. NAS 324 is attached to a phone
tower 323 where each call is received. Preferably, the ARU includes
several ports for processing the individual calls and uses the NAS for
5 voice services. Accordingly, it is NAS 324 that plays and stores all audio
files used by the ACP application to provide automated call processing.
The NAS also provides audio detection for the ARU through DTMF,
tone, and voice recognition. Thus, whereas the NAS provides the audio
interface, the ACP furnishes the data interface. It should be appreciated
10 that in general, calling card calls are typically routed to the ARU via the
ISNAP.

As has been briefly alluded to in the foregoing, the ISNAP
operates as a signaling gateway between the application platforms and
ACD 308 by utilizing appropriate algorithms to determine the call
distribution among the operator positions for the ACD. This process is
15 typically referred to as group selection and, upon completion of the
process, the resulting operator work group is returned to the ACD. The
work group specifies the operator group that is to treat the call, and the
call is subsequently forwarded to the next available console within the
20 selected group to process the call.

In the presently preferred exemplary embodiment, the MTOC --
the manual application platform -- runs operator console applications that

support the Intelligent Services Network (ISN) products. A plurality of T1 Audio channels 311 are provided between an Audio Channel Bank (ACB) 312 and ACD 308, the phone tower 323, and MTOC 328, respectively. The operator console applications use audio interface hardware (not shown in this FIG.) to receive audio via the ACB, and get call data from the ISNAP via an Ethernet network connection. The console identifies incoming calls and, through interaction with ISN databases, provides the necessary scripting and call flow for the operator.

Still continuing to refer to FIG. 3, the ARU is coupled to a Token Ring network 330 which interconnects various telecommunications and processing equipment, e.g., a mainframe computer (MF 332), a Web server 336, and a NIDS server 334 which may also be connected to one of the Ethernet portions provided at the Operator Network Center (ONC). Preferably, the NIDS system is designed to maintain dynamic connections between remote applications and services residing on an ONC LAN. NIDS server 334 provides access to databases and validation service applications via a client/server relationship. Typically, billing data, customer information, service data such as call restriction data, are included in these databases.

In accordance with the teachings of the present invention, a Secure Voice Card (SVC) server 318 is preferably provided as a NIDS node on the Ethernet portion 314A to which the ARU is also connected. Those

skilled in the art should understand upon reference hereto that the SVC server is analogous to the secure card server 108 provided in the network system 100 of FIG. 1, and runs an SVC service application which provides access to an SVC customer profile database 320 for configuration and biometrical validation purposes. The ARU, accordingly, operates as a client to the SVC server with respect to the presently preferred exemplary embodiment of the voice-based validation scheme of the present invention.

The Web server 336 provided in the network 300 operates as a “gateway” towards the PSN portion 338 (e.g., the Internet). A plurality of IP-compatible devices, e.g., T 340A - T 340C, are available for the user 106 to place calls, engage in e-commerce transactions, etc., using his transaction card. Appropriate means such as, e.g., headsets/microphones 341, are also included with the terminals to facilitate interrogation of the user and user voice sampling with respect to the voice-based validation scheme.

The general operation of the voice-based validation scheme for use in the network system 300 described above may now be set forth at this juncture. First, the card user places a calling card-based call in a conventional manner, i.e., the user listens for chime and enters the card number. Thereafter, the user may press the “#” key to bypass the PIN number to enter a voice profile system. Even if the PIN is entered (which

is optional), the scheme may be aware that the user has a voice profile and could optionally require voice-based validation for the transaction being attempted. The system generates a random query from the user's personal profile (i.e., select a single entry among the plurality of entries in the SVC database), prompting the user for input. The user is then required to speak the response or enter appropriate DTMF keys. Card access may be granted for the matching voiceprint, DTMF response, or both. During or after the validation process, the terminating number or its speed-dial number may be entered and, upon subsequent transaction authorization, the call may be connected to the terminating number, whereby upon answering (pick up) a conversation takes place over the voice trunk. Once the system is accessed following authorization, subsequent calls may be made or mis-dialed numbers could be re-dialed without requiring further authentication. That is, only one validation event may be required for a single session which may include several different calls.

FIGS. 4A - 4C depict in greater detail a flow chart of the voice-based validation method described above. When the user places a calling card call (step 402), the ARU answers and prompts the user for the card number (step 404). In response, the user enters the card number, and may optionally enter the PIN or a "#" to immediately bypass the PIN input (step 406). A determination is made if the PIN is entered (decision

block 408) and, if the PIN is not entered, a further determination is made if the SVC profile for the user needs to be accessed (decision block 414). A “*” key may be used for indicating the YES response to enter the voice profile configuration subsystem (block 422) which will be described in further detail hereinbelow with respect to FIG. 5. On the other hand, a “#” may be used to indicate that access to the voice profile configuration subsystem by the user is not desired. Thereafter, the SVC server accesses the SVC database to look up the user profile based on the association between the card indicium (such as, for example, user name, card number assigned by the card issuing entity, PIN, embedded integrated circuit (IC)-based identification, user photograph, and the like) and the user profile (step 416).

If a voice profile for the user is found (decision block 418), the ARU selects a question or item from the profile randomly and queries the user for a response (step 420). On the other hand, if a voice profile for the user is not available, a further determination is made by the system as to whether a voice profile is required (decision block 426). If so, the ARU informs the user that voice profile is needed and, preferably, may prompt the user to access the voice profile configuration subsystem (step 20 424).

Referring back to the decision block 408, if the PIN is entered by the user, another determination is made (decision block 410) as to

whether a voice profile is required for validation. If YES, the flow control of the validation scheme passes to step 416 wherein a voice profile look-up is performed for the card based on card indicia as explained hereinabove. On the other hand, if no voice profile-based validation is required, the ARU simply proceeds to validate the card based on the PIN entry (step 412). If the card is determined to be an invalid card (decision block 430), the flow control returns to step 404 whereby the user is informed that the card is invalid and, subsequently, the ARU prompts the user for another card number or a correct card number.

Referring again to the decision block 426, if the voice profile is not required, however, another determination is made (decision block 428) as to whether a PIN entry is required from the user (that is, whether or not the user previously entered a PIN as determined by the decision block 408). If not, the flow control returns to the path where the ARU proceeds to validate the card based on the PIN entry as determined by the decision block 408. If no PIN has been entered, on the other hand, the decision block 428 determines that a PIN is required and, subsequently, the ARU prompts the user for PIN entry (step 448). If the PIN is entered at this point (decision block 450), the flow control of the validation scheme again passes to step 412 whereby the ARU proceeds to validate the card and its PIN. If, for some reason, the PIN is not entered at this

point, the ARU preferably informs the user that a PIN is required (step 452) and the flow control accordingly goes back to step 404 where by the user is prompted for a new card number entry.

5 Returning to step 420, wherein the ARU selects a question or item from the profile randomly and queries the user for a response, the user accordingly responds by speaking an answer (step 440). Those skilled in the art should realized that the voice profile database may be augmented with DTMF data also and, accordingly, a DTMF response may be entered by the user at this juncture.

10 Upon receiving the voice sample/response from the user, the ARU proceeds to validate the voice sample/response by matching it to a corresponding voiceprint (associated with the question selected for query) in the SVC database (step 442). If a match is found, the user is determined to be a valid user (decision block 444) and the flow control preferably passes to the decision block 428 wherein a determination is made if a PIN is also required. It should be apparent that in some implementations, only voice-based validation may be required, thereby bypassing the PIN entry at this juncture and proceeding directly to the transaction i.e., calling card-based call.

15

20 If the user is determined to be an invalid user per decision block 444, the ARU informs the user that access is denied (step 446) and the

flow control preferably passes to step 404 for prompting the user for another card number or a correct card number.

Returning to block 430, upon validating the user based on voiceprinting and/or PIN entry as described in the foregoing, the flow 5 control passes to the decision block 432 wherein a determination is made as to whether a terminating number (i.e., B-number) is dialed during the validation process. If so, the call is connected to the device/terminal identified by the terminating number (step 438). Otherwise, the ARU issues a double dial tone so that the user may enter the terminating 10 number at this point (step 434). Subsequently, the user dials the complete terminating number or an abbreviated speed dial number (step 436). The call is then connected to that number as set forth in step 438.

Thereafter, the phone conversation (bearer traffic) takes place over 15 the voice trunk (step 454) until disconnected (decision block 456). After getting disconnected, intentionally or otherwise, a billing process is effectuated for computing the toll/charge associated with the call (step 458). If the user presses a redial key (e.g., a “*” key) (decision block 460) or a next call key (e.g., a “#” key) (decision block 462), the flow 20 control returns to step 436, whereby an appropriate terminating number is provided and the call is subsequently connected thereto. This process may take place until the user hangs up the phone. Accordingly, it should

be realized that once the user is validated by the voice profile system for a session, the user may continue to redial or enter other terminating numbers without having to be re-validated for the session.

Referring now to FIG. 5, depicted therein is a flow chart of the 5 voice profile configuration subsystem/process 422 for use in the voice-based validation method described hereinabove. It should be apparent to those skilled in the art that the voice profile configuration/access process may preferably be comprised of a manual access method 500A (user directed method wherein the user enters a pre-defined key) which 10 interfaces with an automated access method 500B (which is directed based on the lack of a user profile) as described hereinbelow.

In a presently preferred exemplary embodiment of the present 15 invention, it is preferably required that a user voice profile database and service node be available, along with a card configuration item that specifies the required use of the database. The user database record definition could be present in the database, or could be built dynamically upon initial entry into the configuration subsystem 422.

In the manual access method 500A, a user profile lookup is performed per card entry key (step 502). If a profile is found (decision 20 block 504), the ARU proceeds with a random query process based on the profile (step 506). After the user speaks an answer in response thereto, the ARU proceeds to validate the user's voice sample based on the SVC

profile (step 508). If the user is determined to be a valid user (decision block 510), the flow control passes to step 512 wherein the ARU prompts the user for PIN input. This step is also reached when the decision block 504 determines that there is no pre-existing voice profile for the user 5 (i.e., the profile needs to be created for the first time in the system). Furthermore, in the presently preferred exemplary embodiment of the present invention, the automated access method 500B also commences with this step (step 512).

After determining that a PIN is entered by the user (decision block 10 514) responsive to the ARU prompting (step 512), the ARU proceeds to validate the card and its PIN (step 516). If the card is determined to be a valid card (decision block 518), the ARU prompts the user for voice samples by directing personalized questions (the order of which may be random for each configuration access) to the user and obtaining 15 appropriate responses therefor. Thereafter, the voice samples are added to the updated SVC profile database (step 526). The user may subsequently complete the configuration process by hanging up the phone terminal used for accessing the configuration subsystem, or by pressing a pre-defined key (e.g., “*”) to return to step 404 in FIG. 4A.

20 If the card is determined to be an invalid card as determined by the decision block 518, the ARU chimes and prompts the user for another card number or a correct card number (step 524). When the user enters

the card number and optional PIN at this point (step 522), the ARU proceeds to validate the card again. The configuration system access process repeats until either a valid card is entered, or the user hangs up.

5 Referring back to the decision block 510 in the manual entry process 500A, if the user is determined to be an invalid user, the ARU informs the user that access is denied (step 520) and prompts for the card number and PIN (step 524) as before. Optionally, the system could initiate a fraud alarm and/or effect a forced hang up in the event of 10 consecutive failed attempts to access the system. Accordingly, when the voice profile is configured for the first time, a card indicium is preferably used for authorizing initial access to the SVC database.

15 Subsequent access to the configuration system, once initialized by the user, will typically only be provided by the manual access method since the automated access method in a preferred embodiment only applies when the system detects an invalid or undefined profile. Also, it should be noted that subsequent access initiated by the user will be gained preferably only through biometric means, i.e., access would not be granted by the card assigned PIN since profile data is available for 20 validation purposes.

Based on the foregoing, it should be appreciated that the present invention advantageously provides a highly effective transaction card

validation system which intimately couples the card with the legitimate user's inherently personal information such as voice samples and other biometric profiles. Those skilled in the art should recognize that the random nature of the user profile query and the unique user voiceprint(s) 5 essentially guarantee that only the legitimate owner can be the card user for any given transaction. Additionally, the user biometric validation method of the present invention is independent of the conventional PIN-based validation methodology, and the teachings of the present invention may be advantageously coupled with other fraud detection mechanisms 10 in order to further enhance security. It should be realized that today's network and server performance, and advanced voice recognition and other biometric pattern recognition technologies permit fairly rapid access times for the card validation scheme of the present invention.

Those skilled in the art should further appreciate that both card- 15 issuing companies and their customers benefit from the card validation scheme described herein. The cost savings realized due to fraud prevention will balance any delays in access times, and customers can justify the card access overhead by the added comfort that their card is secure at all times -- they would no longer have to worry about losing a 20 card, remembering a PIN, or having to conceal a card number and its PIN in a wallet or other personal effect(s), or have to deal with any fraud aftermath. Moreover, because the profiles can be modified periodically

or each time the card is used for a transaction with new options/responses, card access security is further buttressed.

It is believed that the operation and construction of the present invention will be apparent from the foregoing Detailed Description.

5 While the method and system shown and described have been characterized as being preferred, it should be readily understood that various changes and modifications could be made therein without departing from the scope of the present invention as set forth in the following claims. For example, although the presently preferred 10 exemplary embodiment of the present invention has been described as an active fraud prevention system, it is possible to implement the present invention in a passive mode, i.e., as an auxiliary system which would intervene only in the event of fraud detection by an existing system. In such a scenario, the validation system of the present invention would 15 query the user to verify access only when fraud is suspected.

In addition, while the voice-based validation scheme for a calling card transaction has been particularly exemplified hereinabove, it should be apparent to those skilled in the art upon reference hereto that the 20 teachings of the present invention may be advantageously practiced in the context of accessing personal information such as a bank account, employment records, medical records, credit reports, or private club membership materials, e-commerce accounts, brokerage accounts, and

PATENT APPLICATION
DOCKET NO.: 1275-0006
COS-99-070

the like. Accordingly, it should be clearly understood that these and other variations, substitutions, additions, re-arrangements and modifications are contemplated to be within the ambit of the present invention whose scope is solely limited by the claims set forth below.

WHAT IS CLAIMED IS:

- 1 1. A method of validating a user for a transaction to be
2 effectuated by using a transaction card, comprising the steps of :
3 configuring a biometric profile for said user, said biometric
4 profile including a plurality of biometric samples relating to said user;
5 associating said biometric profile with an indicium assigned
6 to said transaction card;
7 biometrically interrogating said user when said transaction
8 is attempted by said user;
9 monitoring a biometric response generated with respect to
10 said user in response to said step of biometrical interrogation;
11 determining if said biometric response matches a biometric
12 sample in said biometric profile; and
13 if so, approving said user for said transaction.

1 2. The method of validating a user for a transaction as set forth
2 in claim 1, wherein at least a portion of said plurality of biometric
3 samples comprises voice samples generated by said user responsive to a
4 plurality of questions directed to said user in said configuring step, and
5 further wherein said step of biometrical interrogation involves querying
6 said user for a voice response to a randomly selected question of said
7 plurality of questions.

1 3. The method of validating a user for a transaction as set forth
2 in claim 1, further comprising the steps of:

3 prompting said user to input said indicium assigned to said
4 transaction card after determining that said biometric response matches
5 a biometric sample of said biometric profile;

6 determining if said indicium is a valid personal
7 identification number operating as a password associated with said
8 transaction card; and

9 denying access to said user for said transaction if said
10 indicium is not a valid personal identification number associated with
11 said transaction card.

1 4. The method of validating a user for a transaction as set forth
2 in claim 1, further comprising the steps of:

6 confirming that said indicium is a valid personal
7 identification number associated with said transaction card; and

1 5. The method of validating a user for a transaction as set forth
2 in claim 1, wherein the step of configuring a biometric profile for said
3 user is effectuated manually.

1 6. The method of validating a user for a transaction as set forth
2 in claim 1, wherein the step of configuring a biometric profile for said
3 user is effectuated automatically.

1 7. The method of validating a user for a transaction as set forth
2 in claim 1, further comprising the step of updating said biometric profile
3 for said user.

1 8. A method of validating a user for a call to be effectuated
2 over a Public Switched Telephone Network (PSTN) using a calling card,
3 comprising the steps of:

4 configuring a personalized profile for said user, said
5 personalized profile including a plurality of voice samples elicited from
6 said user in response to a plurality of personalized questions directed to
7 said user;

8 associating said personalized profile with an indicium
9 assigned to said calling card;

10 determining if a voice verification is needed with respect to
11 said user when said call is attempted by said user;

12 if so, querying said user for a voice response to a question
13 that is randomly selected from said plurality of personalized questions;

14 verifying if said voice response matches a corresponding
15 voice sample in said voice profile; and

16 if so, approving said user for said call involving said calling
17 card.

1 9. The method of validating a user for a call as set forth in
2 claim 8, further comprising the steps of:

3 populating at least a portion of said personalized profile
4 with a plurality of Dual Tone Multi Frequency (DTMF) sample
5 responses elicited from said user in said configuration step;

6 prompting said user to input a DTMF response in response
7 to said question that is randomly selected from said plurality of
8 personalized questions;

9 verifying if said DTMF response matches a corresponding
10 sample response in said personalized profile; and

11 denying access to said user for said call if said DTMF
12 response does not match said corresponding sample response in said
13 personalized profile.

1 10. The method of validating a user for a call as set forth in
2 claim 8, further comprising the steps of:

3 prompting said user to input said indicium assigned to said
4 calling card after verifying that said voice response matches a
5 corresponding voice sample in said voice profile;

6 determining if said indicium is a valid personal
7 identification number associated with said calling card; and

8 denying access to said user for said call if said indicium is
9 not a valid personal identification number associated with said calling
10 card.

1 11. The method of validating a user for a call as set forth in
2 claim 8, further comprising the steps of:

3 prompting said user to input said indicium assigned to said
4 calling card after verifying that said voice response does not match a
5 corresponding voice sample in said voice profile;

6 confirming that said indicium is a valid personal
7 identification number associated with said calling card; and

8 approving said user for said call upon said confirmation.

1 12. A fraud prevention method for use in a transaction-card-
2 based system having a conventional authentication process, said
3 comprising the steps of:

4 determining, by utilizing said conventional authentication
5 process, if a fraudulent transaction is being attempted in said transaction-
6 card-based system by a user using a transaction card;

7 if so, biometrically interrogating said user to obtain a
8 biometric sample from said user; and

9 upon obtaining said biometric sample, denying access to
10 said user for said transaction in said transaction-card-based system if said
11 biometric sample does not match an entry stored in a biometric profile
12 database inherently associated with said transaction card's owner.

1 13. The fraud prevention method for use in a transaction-card-
2 based system as set forth in claim 12, wherein said fraudulent transaction
3 is selected from the group consisting of: placing a calling card call,
4 accessing personal information data, accessing a bank account, accessing
5 an Internet account, accessing a credit report, accessing employment
6 records, and accessing medical records.

PATENT APPLICATION
DOCKET NO.: 1275-0006
COS-99-070

1 14. The fraud prevention method for use in a transaction-card-
2 based system as set forth in claim 12, wherein said entry inherently
3 associated with said transaction card's owner comprises a voiceprint
4 associated with said owner.

1 15. The fraud prevention method for use in a transaction-card-
2 based system as set forth in claim 12, wherein said entry inherently
3 associated with said transaction card's owner comprises at least one of
4 a fingerprint, retinal scan, palm print, and implanted ID chip associated
5 with said owner.

1 16. An access control system for use with a transaction-card-
2 based scheme, said system comprising:

3 a network operable with a terminal, said terminal for
4 interacting with a user in association with a transaction card;

5 a controller disposed in the network to query said user when
6 said user attempts a transaction using said transaction card;

7 a server disposed in the network, said server responding to
8 messages from said controller with respect to querying said user; and

9 a profile database coupled to said server, said profile
10 database having a plurality of biometric samples inherently coupled to
11 said user, wherein said biometric samples are associated with an
12 indicium assigned to said transaction card such that when said user
13 attempts said transaction, said controller queries said user for a response
14 thereto and if said response does not match a corresponding entry in said
15 profile database, access is denied to said user for said transaction.

1 17. The access control system for use with a transaction-card-
2 based scheme as set forth in claim 16, wherein said entry inherently
3 coupled to said user comprises at least one of a fingerprint, retinal scan,
4 palm print, and implanted ID chip associated with said user.

1 18. The access control system for use with a transaction-card-
2 based scheme as set forth in claim 16, wherein said entry inherently
3 coupled to said user comprises a voiceprint associated with said user.

1 19. The access control system for use with a transaction-card-
2 based scheme as set forth in claim 16, wherein said controller comprises
3 an Automated Response Unit associated with a Public Switched
4 Telephone Network.

1 20. The access control system for use with a transaction-card-
2 based scheme as set forth in claim 16, wherein said terminal comprises
3 a wireline phone.

1 21. The access control system for use with a transaction-card-
2 based scheme as set forth in claim 16, wherein said terminal comprises
3 an Internet phone.

1 22. The access control system for use with a transaction-card-
2 based scheme as set forth in claim 16, wherein said terminal comprises
3 a wireless medium device.

ABSTRACT OF THE DISCLOSURE

A validation scheme for use with a transaction card such as a calling card, et cetera, using personalized biometric profile data that is inherently coupled to the card owner/user. A configuration process is used for populating a profile database with sample voice or other biometric responses elicited from the owner/user in response to a plurality of questions relating to information uniquely linked to the user such as, e.g., name, age, hobbies, et cetera, or biometric responses such as fingerprints, retinal scans, and palm prints, or implanted ID chips. When a transaction is attempted using the transaction card, a determination is made if a voice profile validation is required for authentication. If so, a question from the plurality of questions used in the configuration process is randomly selected and directed to the user for a response. Access is provided only if a match between the response and corresponding sample is found. In a passive mode, the validation scheme may be utilized as an auxiliary fraud prevention scheme in addition to existing authentication systems.

Fig. 1

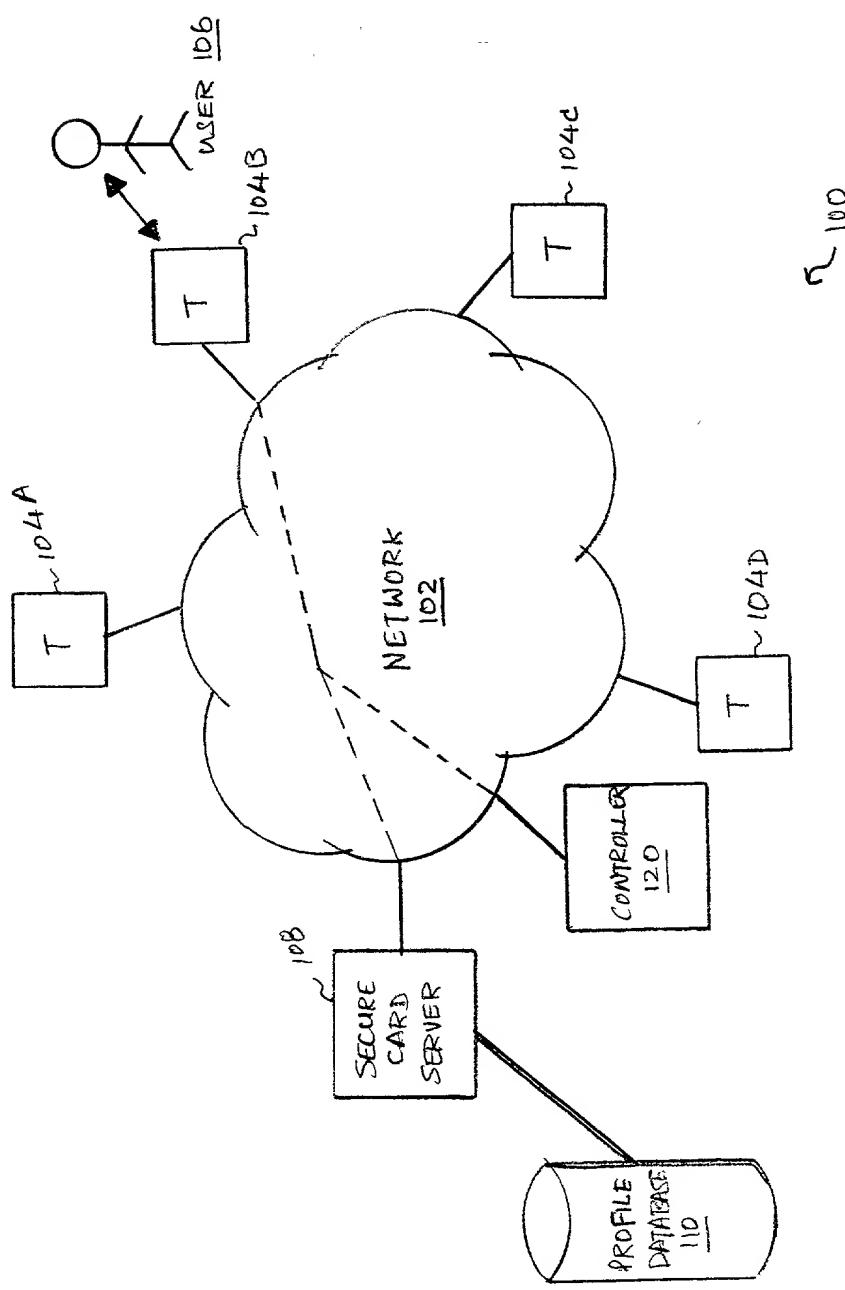
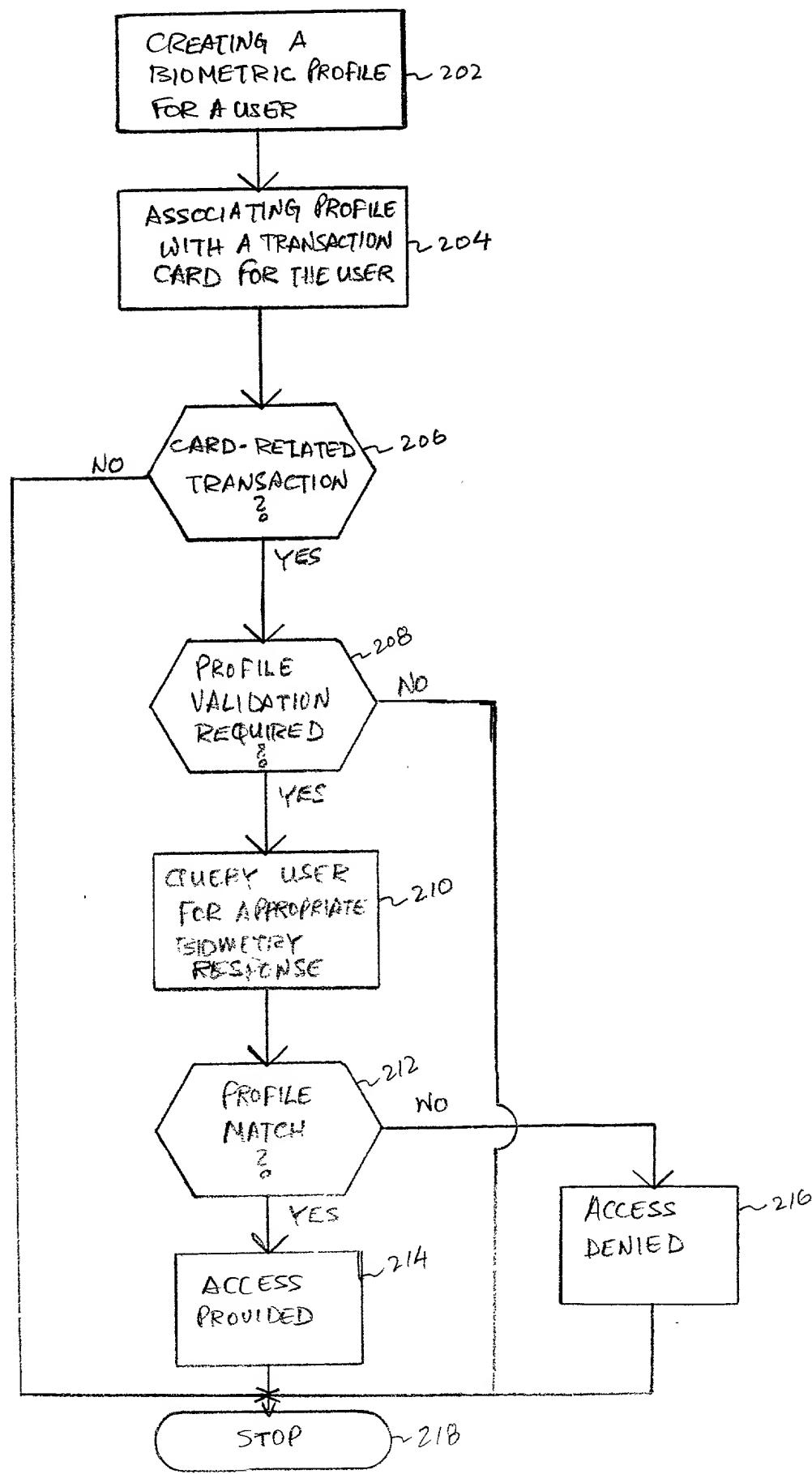


FIG.2



1275-0006

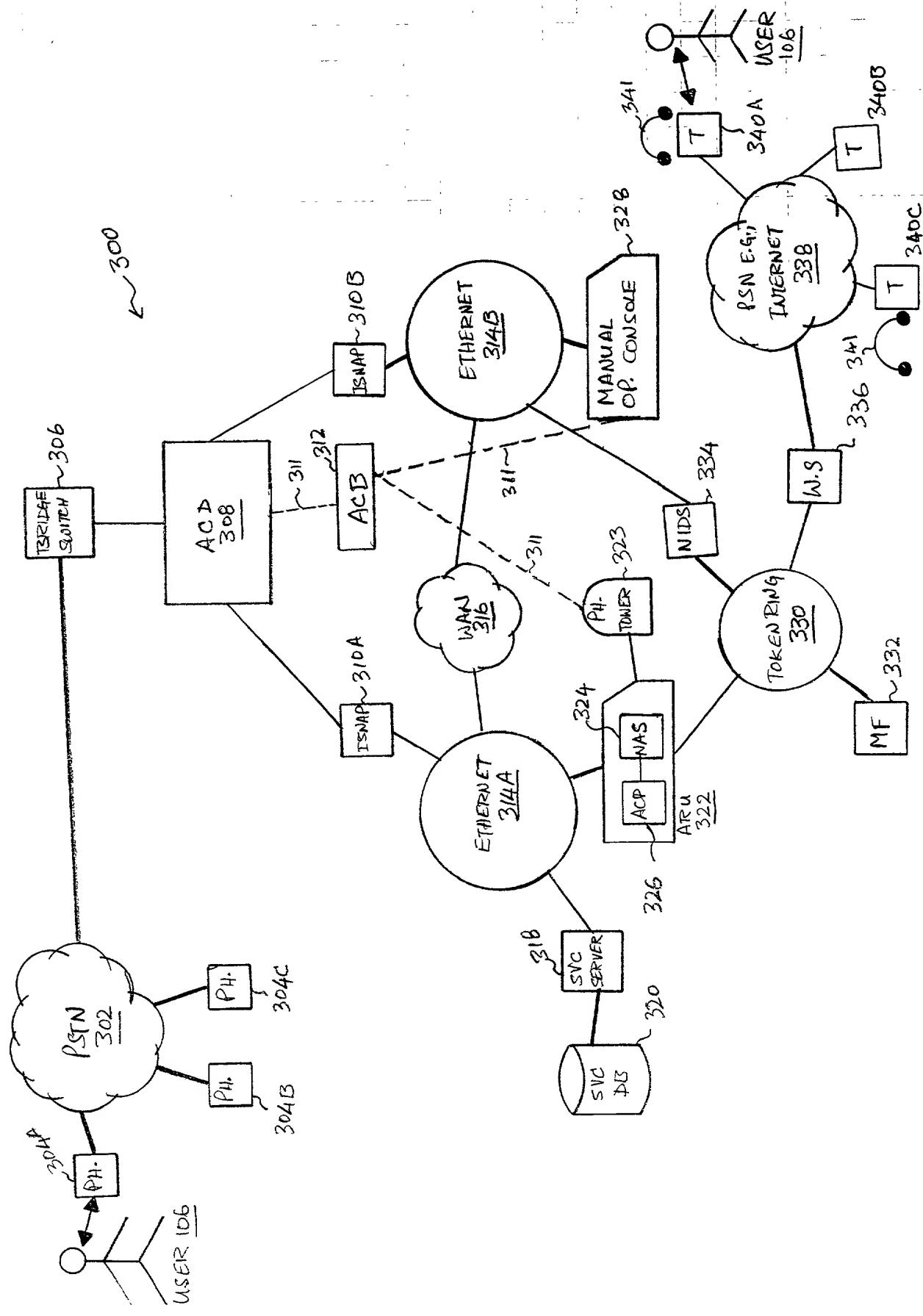


Fig. 3

FIG. 4A

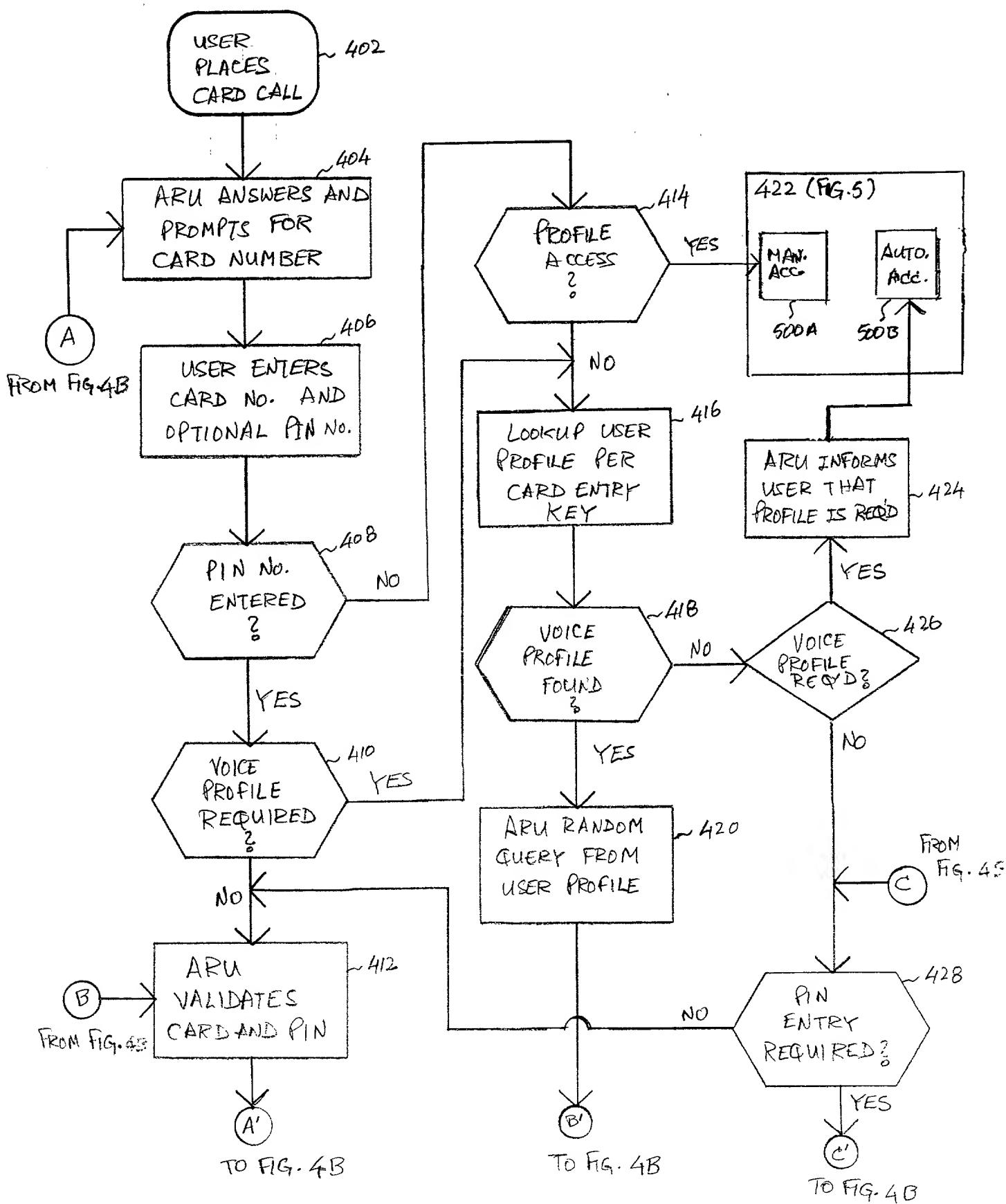
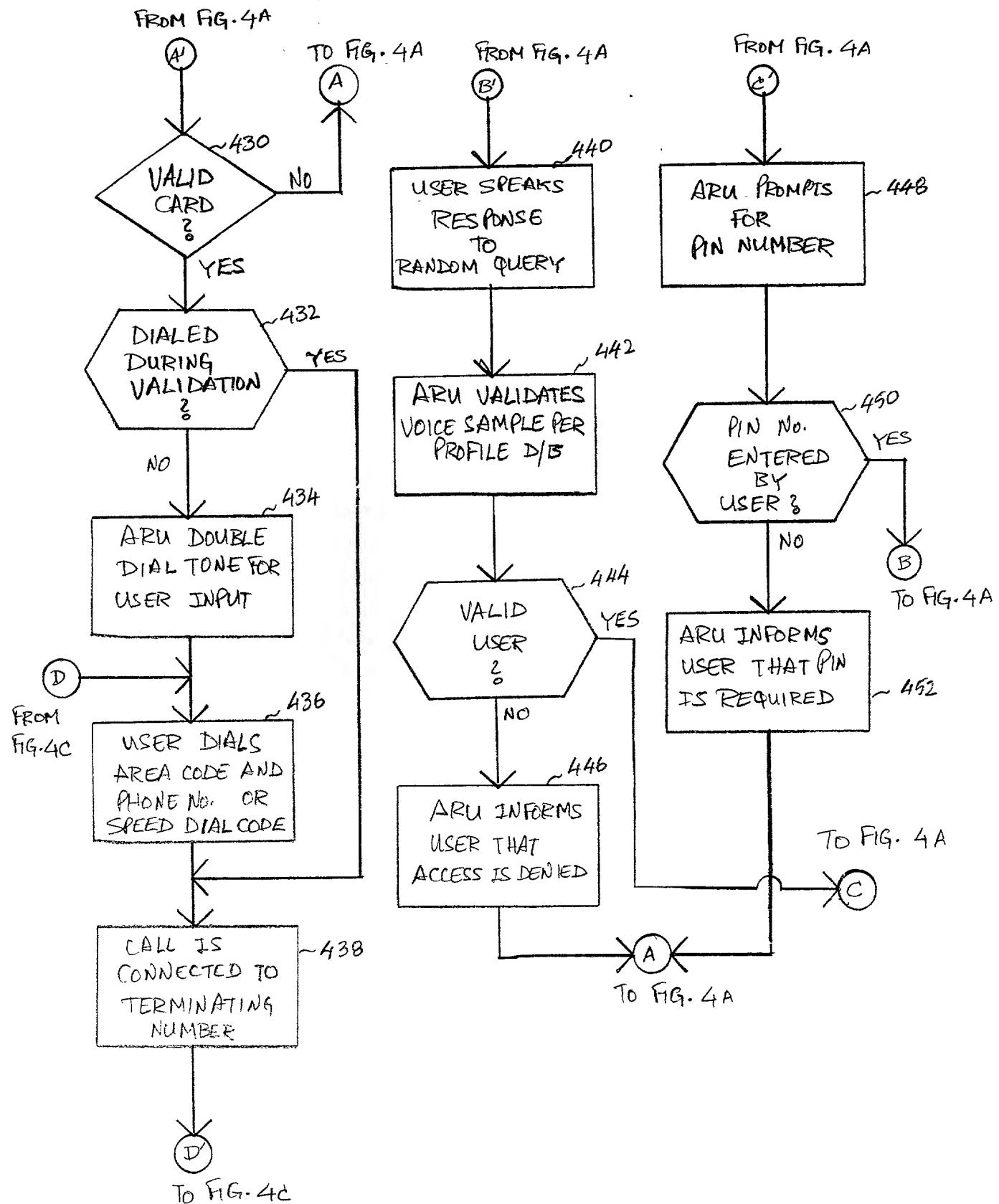


FIG. 4B



1275-0006

FIG. 4C

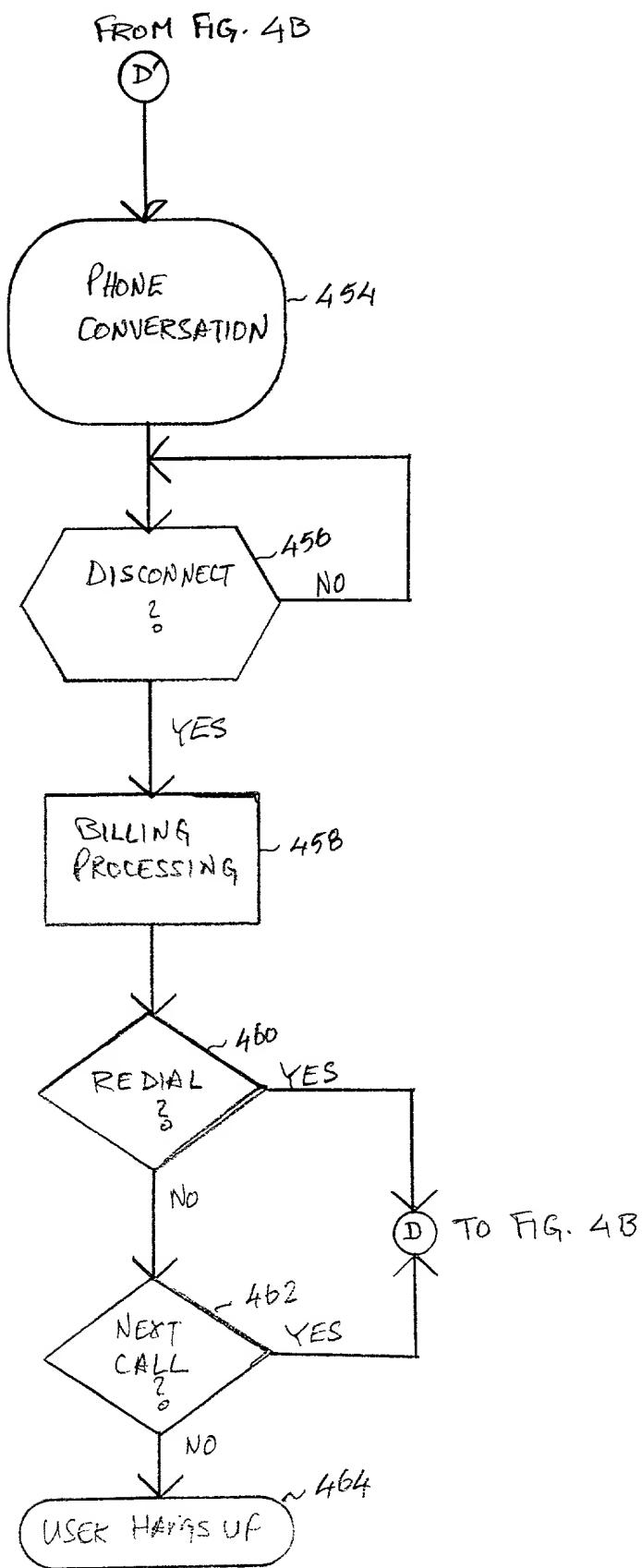
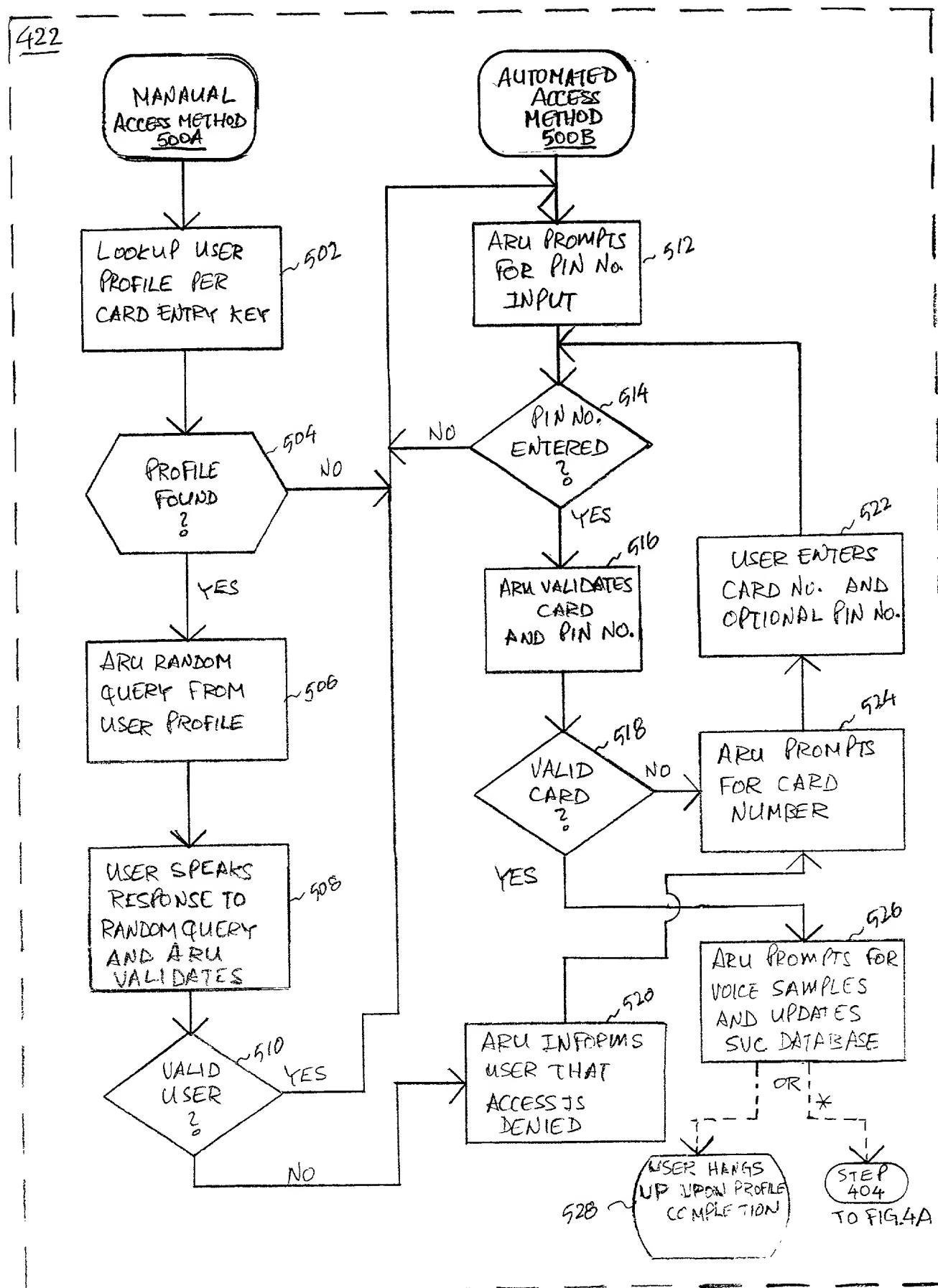


FIG. 5



**DECLARATION AND POWER OF ATTORNEY
FOR UTILITY PATENT APPLICATION**

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SECURE TRANSACTION CARD USING BIOMETRICAL VALIDATION

the specification of which

is attached hereto
 was filed on _____ as Application Serial No.
and was amended on _____

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above. I do not know and do not believe that the same was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof of more than one year prior to this application, and said invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months prior to this application.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, Section 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code §119 (a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)

(number) (country) (date filed)

Priority Claimed

yes no

(number)

(country)

(date filed)

yes no

(number)

(country)

(date filed)

I hereby claim the benefit under Title 35, United States Code§119(e) of any United States provisional application(s) listed below.

(Application Number(s)) (Filing Date mm/dd/yy)

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) or Section365(c) of any PCT international application designating the United States of America, listed below, and insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

(Application Serial No.) (Filing date) (Status)

I hereby appoint Carl Evans, Reg. No. 33,874; Deborah Miller, Reg. No. 37,679; Paul A. Roberts, Reg. No. 40,289; my attorneys and Frank McKiel, Reg. No. 43,792; Satheesh Karra, Reg. No. 40,246 my patent agents with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to:
Technology Law Department
MCI WORLDCOM, Inc.
1133 19th STREET NW
WASHINGTON, D.C. 20036

Direct Telephone Calls To:
(719) 535-1451

I hereby declare that all statements made herein of my knowledge are true and that all statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of Sole or First Inventor:
P.O/Residence Address:

Thomas J. Herder
1124 26th St. Ct., NW, Cedar Rapids, IA 52405

Citizenship: USA

Signature: Thomas J. Herder Date: 7/26/00